UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/708,825	03/26/2004	Blayn W. Beenau	60655.8600	2824

20322 7590 05/11/2006

SNELL & WILMER
ONE ARIZONA CENTER
400 EAST VAN BUREN
PHOENIX, AZ 85004-2202

EXAMINER	
WALSH, DANIEL I	
ART UNIT	**PAPER NUMBER**
2876	

DATE MAILED: 05/11/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/708,825	BEENAU ET AL.	
	Examiner	Art Unit	
	Daniel I. Walsh	2876	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *10 March 2006*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-56* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-56* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. Receipt is acknowledged of the Amendment received on 10 March 2006.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

This application currently names joint inventors. In considering patentability of the claims under 35 U.S.C. 103(a), the examiner presumes that the subject matter of the various claims was commonly owned at the time any inventions covered therein were made absent any evidence to the contrary. Applicant is advised of the obligation under 37 CFR 1.56 to point out the inventor and invention dates of each claim that was not commonly owned at the time a later invention was made in order for the examiner to consider the applicability of 35 U.S.C. 103(c) and potential 35 U.S.C. 102(e), (f) or (g) prior art under 35 U.S.C. 103(a).

2. Claims 1-15 and 19-48, 50-51, 53-54, and 56 are rejected under 35 U.S.C. 103(a) as being unpatentable over Black, as discussed above.

Re claim 1, Black teaches a transponder configured to communicate with a reader, a reader configured to communicate with the system, a fingerprint sensor to detect a fingerprint sample, the fingerprint sample configured to communicate with the system (FIG. 1A). Though silent to a verification device to verify the sample, the Examiner notes that a transaction is

authorized upon verification of the sample. Therefore, at the time the invention was made, it would have been obvious to have a verification device in order to verify the sample as part of the authentication (security).

Re claim 2, the Examiner notes that the sensor communicates with the system via at least one of a transponder, reader, and network (FIG. 1A).

Re claim 3, it is understood that the biometric sensor is configured to facilitate a finite/limited number of scans (one for example) in order to receive a sample.

Re claim 4, FIG. 5A+ shows that the fingerprint sensor logs at least one of a detected fingerprint sample, processed sample, and stored sample.

Re claims 5-6, Black teaches (col 6, lines 56+) that the customer record can be stored locally or remotely. The Examiner notes that though Black is silent to a datapacket stored on a database, Black teaches that the customer record can include biometric information, user information, etc. (FIG. 5A+ for example). Therefore, the Examiner notes that it would be within the skill in the art for such a collection of data can be interpreted as a data packet. It would have been obvious to store such information on a database, in order to have a well known and conventional means of storing data for quick retrieval and organization. It has been discussed above that the data can be stored remotely or locally. Accordingly, it would have been obvious to one of ordinary skill in the art to store it on the transponder or a remote device based on security needs.

Re claim 7, it has been discussed above that samples are received and stored for providing security/authentication. It would have been obvious that the samples would be received by an authorized receiver in order to ensure security and reliability.

Re claim 8, though silent to capacitive/optical scanner, the Examiner notes that such means are well known and conventional in the art to receive a fingerprint sample. One would have been motivated to use such a scanner in order to obtain an accurate sample.

Re claim 9, the Examiner notes that such fingerprint minutia detection/verification is well known and conventional in the art for accurate identification of a sample.

Re claim 10, such limitations are well known among fingerprint sensors. One would have been motivated to use such detection means, to verify that the finger/sample is real/living.

Re claim 11, the Examiner notes that the proffered sample is compared to a stored/registered sample to see if there is a match (abstract).

Re claim 12, it has been discussed above that a comparison is performed. The Examiner notes that it would have been obvious to one of ordinary skill in the art to use a microprocessor/controller/processor (interpreted as a protocol/sequence controller) to electronically perform the comparison, in order to have an electronic (automated) means to quickly and reliably perform the comparison, as is conventional in the art.

Re claim 13, the Examiner notes that as a sample is stored, it's interpreted as registered.

Re claim 14, Black teaches that a customer's account is linked to the biometric data, and can be used for payment and is linked to a credit or debit account (abstract, col 6, lines 46+).

Re claim 15, the Examiner notes that it is obvious that the system of Black would be used by a plurality of customers. As such, it would have been obvious that different people have different samples, which would be associated with their different accounts.

Re claim 19, though Black is silent to the sensor providing notification upon detection of a sample, the Examiner notes that it is well within the skill in the art to provide notification that a

sample ahs been detected, in order to provide indication to the user, that the sample was received and they don't have to keep offering a sample. As Black indicates when a sample has been authorized (transaction allowed) it would have been obvious to indicate when the sample is read/detected as a means to provide guiding information to the user. Additionally, the Examiner notes that the mere authorization of a transaction can be broadly interpreted as providing notification upon detection of a sample because authorization cannot occur unless the sample was detected.

Re claim 20, it has been discussed above that the device facilitates a financial transaction.

Re claims 21 and 34, though silent to secondary security procedures, the Examiner notes that such procedures such as PINs, codes, passwords, etc. are well known and conventional in the art. One would have been motivated to use such procedures for increased security.

Re claim 22, Black teaches a method for facilitating biometric security in a transponder/reader system comprising providing a fingerprint to a fingerprint sensor communicating with the system to initiate verification of a fingerprint sample for facilitating authorization of a transaction (abstract).

Re claim 23, the Examiner has interpreted the storing of the fingerprint sample with the system as an authorized sample receiver.

Re claim 24, registering includes proffering a fingerprint (abstract, FIG. 5A).

Re claim 25, the limitations have been discussed above re claim 8.

Re claim 26, Black teaches that a sample is stored and that proffered samples are compared and verified to complete a transaction (abstract).

Re claim 27, Black teaches the step of proffering a biometric to a sensor communicating with the system to initiate verification, as discussed above. As discussed above, Black teaches that the information can be stored on the transponder itself or remotely, depending on the desired security. Though silent to a database, a database is an obvious expedient as discussed above. Accordingly, it would have been obvious to process database information contained in at least one of the transponder, reader, sensor, server, and reader system as a means to authenticate/verify a user.

Re claim 28, Black teaches comparing the proffered sample with stored sample (abstract).

Re claim 29, Black teaches (FIG. 4A, for example) that a registration processor and print processor are used. It would have been obvious to one of ordinary skill in the art to use a processor to compare the fingerprint samples in order to provide an automated means to accurately verify a sample, as is conventional in the art.

Re claims 30-32, the limitations have been discussed above re claims 8-10

Re claim 33, the Examiner notes that as the system is used with more than one user (therefore more than one sample) it would have been obvious to detect/process/sore a second fingerprint sample (of additional users).

Re claim 35, the limitations have been discussed above.

Re claim 36, Black teaches that the sample is detected at a sensor configured to communicate with the system via one of a transponder/reader/network (FIG. 1A-1C).

Re claim 37, the limitations have been discussed above re claims 8-10.

Re claim 38, Black teaches detecting/storing/processing the sample (abstract).

Re claim 39, the Examiner notes that it would have been obvious to receive a finite/limited number of fingerprints during a transaction (abstract), namely, one, for example, for a transaction.

Re claim 40, the examiner notes that it is obvious that the fingerprint samples are logged/stored at least temporarily, in order for them to be verified (stored in a buffer for example during comparison). Additionally, the Examiner notes that storing/logging signatures, transaction details, signatures associated with a transaction (more permanently then in a buffer) are well known and conventional in the art for record keeping purposes/security.

Re claim 41, as discussed above, it would have been obvious to one of ordinary skill in the art to detect/process/store a second sample, when the system is used by different people with different accounts and samples.

Re claim 42, the limitations have been discussed above re claims 8-10.

Re claim 43, the comparison of a proffered sample to a stored/registered sample has been discussed above.

Re claim 44, the limitations have been discussed above re claims 8-10.

Re claim 45, the Examiner notes that the proffered biometric is indeed compared with a sample of at least one of a criminal, terrorist, and card member, as the sample is compared to a current card members sample, to authorize the transaction.

Re claim 46, verifying the sample using information contained on one of a local database/remote database/third party controlled database would have been an obvious expedient in instances where the data is stored remote from the transponder. The fingerprint would be

verified by using information contained in a database, as a preferred means to organize data for efficient and easy storage and retrieval (remote or local).

Re claim 47, the verification of a sample using a protocol/sequence controller (interpreted as a processor) has been discussed above.

Re claims 1, 22, and 35, Black is silent to determining that the sample is associated with preset transaction limitation/in compliance.

Baer teaches such limitations (paragraph [0037]).

At the time the invention was made, it would have been obvious to one of ordinary skill in the art to combine the teachings of Black with those of Baer.

One would have been motivated to do this to have different security levels.

Re claim 48, Baer teaches a maximum transaction amount, as discussed above.

Re claim 50, though silent to a government or third party storing the biometrics, Black as discussed above, teaches storing the biometrics remotely. Accordingly, the Examiner notes it would have been obvious to one of ordinary skill in the art to store the samples by a government agency or third party in order to securely store the samples, as they are critical data associated with accounts and finance, security is desired.

Re claims 51 and 53, the limitations have been discussed above re claims 48 and 50 respectively.

Re claims 54 and 56, the limitations have been discussed above re claims 48 and 50, respectively.

3. Claims 15, 33, 41 are rejected under 35 U.S.C. 103(a) as being unpatentable over Black/Baer, as discussed above in view of Martizen et al. (US 2002/0191816).

The teachings of Black/Baer have been discussed above.

Black/Baer is silent to different samples (of the same person) associated with different one of personal information, credit card information, etc. as claimed.

Martizen et al. teaches different registered biometric samples are associated with different personal information (different fingers with different accounts) (FIG. 6A).

At the time the invention was made, it would have been obvious to one of ordinary skill in the art to combine the teachings of Black/Baer with those of Martizen et al.

One would have been motivated do to this to permit multiple accounts to be security accessed with different samples, for user convenience and security.

4. Claim 16 is rejected under 35 U.S.C. 103(a) as being unpatentable over Black/Baer as discussed above, in view of Moebs et al (US 2005/0065872).

The teachings of Black/Baer have been discussed above.

Black/Baer are silent to primary and secondary associating.

The Examiner notes that such associating is well known in the art (line of credit, for example). Specifically, Moebs et al. teaches that a customer can avoid overdraft by preauthorizing the financial institution to tie the customers' checking account to one or more of the customers other accounts (paragraph [0017]).

At the time the invention was made, it would have been obvious to one of ordinary skill in the art to combine the teachings of Black/Baer with those of Moebs et al.

One would have been motivated to do this in order to provide for overdraft protection, for example.

5. Claim 17 is rejected under 35 U.S.C. 103(a) as being unpatentable over Black/Baer in view of Teicher (US 6,257,486).

Black/Baer is silent to mutual authentication upon verification of the biometric sample.

The Examiner notes that mutual authentication is well known and conventional in the art, as a security measure, to ensure that a valid reading device and device are communicating. It would have been obvious to one of ordinary skill in the art to authenticate upon verification of the sample, in order to ensure that the transponder and reader are authentic and authorized to communicate with each other. Specifically, Teicher teaches a contactless smart card that being mutual authentication after an input (PIN) is entered (col 7, lines 35+).

At the time the invention was made, it would have been obvious to one of ordinary skill in the art to combine the teachings of Black/Baer with those of Teicher.

One would have been motivated to do this in order to employ well known security measures.

6. Claim 18 is rejected under 35 U.S.C. 103(a) as being unpatentable over Black/Baer in view of Goodman (US 2002/0043566).

The teachings of Black/Baer have been discussed above.

Black teaches that the transaction is blocked when the biometrics do not match, as is conventional in the art, but Black is silent to deactivation upon rejection of the sample.

The Examiner notes that it is well known and conventional in the art for card to be disabled, as a security measure, if a predetermined amount of failed attempts are detected, for example. Specifically, Goodman et al. teaches deactivation of a card if a predetermined amount of incorrect PIN attempts are detected (paragraph [0029]).

At the time the invention was made, it would have been obvious to one of ordinary skill in the art to combine the teachings of Black with those of Goodman et al.

One would have been motivated to do this in order to increase system security.

Though Goodman et al. is silent to a biometric input, the Examiner notes that Goodman et al. is relied upon for teaching disabling of access when a matching input is not received. It would have been obvious to disable the transponder when biometrics don't match (biometrics replacing PIN input, as a more secure alternative).

7. Claims 4, 21, 34, and 40 are rejected under 35 U.S.C. 103(a) as being unpatentable over Black/Baer, as discussed above, in view of Black (US 2005/0122209).

The teachings of Black/Baer have been discussed above.

Re claims 21 and 34, Black is silent to secondary security procedures. Re claims 4 and 40, Black is silent to logging each proffered fingerprint sample.

Black '209 teaches such procedures through signature verification (abstract). Black '209 teaches storing of digital and electronic signature for record keeping purposes (paragraph [0125]).

At the time the invention was made, it would have been obvious to one of ordinary skill in the art to combine the teachings of Black/Baer with those of Black '209.

One would have been motivated to do this for increased security and record keeping purposes.

8. Claims 49, 52, and 55 are rejected under 35 U.S.C. 103(a) as being unpatentable over Black/Baer, as discussed above, in view of Wallace (US 5,988,497).

The teachings of Black/Baer have been discussed above.

Black/Baer are silent to a second sample to override a transaction limitation.

Wallace teaches multiple tiers of authentication in order to authenticate a transaction that meets certain conditions (abstract).

At the time the invention was made, it would have been obvious to one of ordinary skill in the art to combine the teachings of Black/Baer with those of Wallace.

One would have been motivated to do this to provide more authentication for certain transactions, as it is known that additional samples can provide more security. The replacing of additional PINs of Wallace, by biometrics of Black is an obvious expedient to provide more secure transactions.

Response to Arguments

9. Applicant's arguments with respect to the claims have been considered but are moot in view of the new ground(s) of rejection. The Applicants amendment has set forth limitations to the independent claims regarding association of a fingerprint/sample with a transaction limitation. The Examiner has cited the art to Baer, as discussed above to address this limitation, and has cited Wallace to teach additional layers of security (re claims 49, 52, and 55).

10. Regarding the newly added dependent claims 48-56, these limitations are deemed obvious in light of the prior art as discussed above.

Additional Remarks

11. As an example, Janiak et al. (US 2002/0097142) teaches user indication. User indication is well known in the art to keep the user informed during a process. Typical user indication is readily seen at checkouts/point of sale devices, for example.

McCall et al. (US 2003/0132297) stores/logs signatures, Haala et al. (US 2005/0102524) teaches recording details is authentication fails and Segal et al. (US 2002/0066784) teaches bundling a signature with transaction database to effect proof of a transaction.

Hoshino et al. (US 6,636,620) teaches capacitive sensors detecting ridges and valleys, Kamei (US 5,901,239) teaches bifurcation and other features, and Tuli (US 5,942,761) teaches detection of body heat with fingerprints. The Examiner notes that the type of sensor devices claimed are well known and conventional in the art of fingerprint detection and authentication.

The Examiner notes that PINs associated with biometrics are well known and conventional for increased security (versus just a biometric; see US 2001/0029493, 5,764,789, 2004/0084524, 2002/0174067, 2002/0062284, 2001/0018660, which show that a PIN and biometric can be used together, for additional security over just a PIN or biometric, for example). The Examiner also notes Royer et al. (US 2004/0155101) teaches the use of different biometrics with multiple accounts and Ramachandran (US 2001/0013551) and Pitroda (US 6,925,439) which teach consolidation of card accounts onto one card for convenience and the selection of an account from a plurality of accounts.

The Examiner notes that different levels of security are well know and conventional in the art. For example, Deo et al. (US 5,721,781) teaches based on transaction amounts, different information is required in order to provide security/assurance that the user is valid (see Fig. 9), Rasmussen et al. (US 6,834,795) teaches similar teachings (FIG. 5), and Tetro et al. (US 6,095,413) teaches added security trough use of a separate databases).

Conclusion

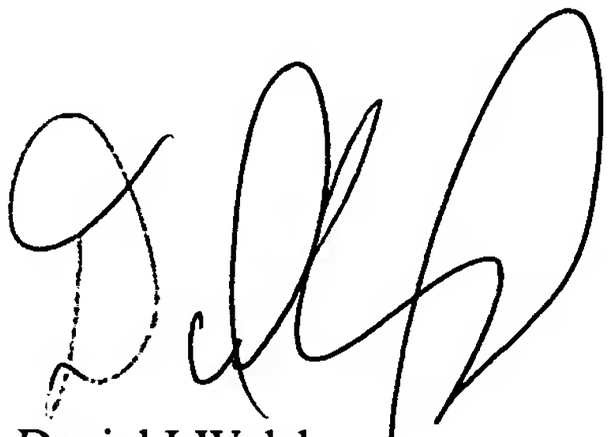
12. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Daniel I. Walsh whose telephone number is (571) 272-2409. The examiner can normally be reached on M-F 7:30-4:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Michael G. Lee can be reached on (571) 272-2398. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).



Daniel I Walsh
Examiner
Art Unit 2876
5-3-06